RFC-0014 FedRAMP 20x Phase Two Key Security Indicators

RFC Front Matter

- **Status:** Open
- **Created By:** FedRAMP
- **Start Date:** 2025-09-10
- **Closing Date:** 2025-10-10
- **Short Name:** rfc-0014-phase-two-ksis

Where to Comment

Members of the public may submit multiple different comments on different issues during the public comment period. The public is asked to please refrain from including documents or spreadsheets (especially those with in-line comments or suggested changes) in public comment as this creates a significant additional review burden.

Formal public comment for official consideration by FedRAMP can be made via the following mechanisms in order of preference:

1. GitHub Post: https://github.com/FedRAMP/community/discussions/83
2. Public Comment Form: https://forms.gle/Ry25zn1GUDJXHs5o9
3. Email: pete@fedramp.gov with the subject "**RFC-0014 Feedback**"

Note: FedRAMP will review and publicly post all public comments received via email, but will not otherwise respond. Email submissions from federal agencies will only be made public when requested by the agency.

Summary & Motivation

FedRAMPs Key Security Indicators summarize the security capabilities expected of a cloud service provider who wishes to obtain and maintain a FedRAMP 20x authorization. These capabilities are broadly summarized with the expectation of broad automated application.

This RFC summarizes proposed changes to the existing Key Security Indicators where they were ineffective, unclear, or insufficient. This RFC also proposes new Key Security Indicators for both FedRAMP Low and FedRAMP Moderate to resolve outstanding gaps and integrate additional controls.

Keen observers will note that there are very few new Key Security Indicators required for Moderate; this is because almost every single Moderate control is already covered by an existing or slightly modified Key Security Indicator. Cloud service providers seeking Moderate authorization during the Phase Two pilot will need to demonstrate _significantly_ approved maturity in both depth and automation related to all Key Security Indicators; simply adopting the new Key Security Indicators will not be sufficient.

During Phase One FedRAMP would accept written attestation that some Key Security Indicators were met for a Low authorization. During Phase Two, FedRAMP will expect truly automated and opinionated validation of Key Security Indicators for a Moderate authorization. For example, KSI-PIY-06 expects validation that a provider has staff and budget for security - FedRAMP accepted attestations about general budget or staffing numbers for Low but will expect to see automated validations demonstrating the participation and involvement of security staff in common operations to prove this validation is met for Moderate.

For this and other Key Security Indicators, FedRAMP plans to publish simple Technical Assistance prior to accepting submissions for Phase Two. In the interim, the FedRAMP Community 20x Pilot Review Feedback Friday discussion contains many pro-tips for navigating Key Security Indicators.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Retired Key Security Indicators & Validations

The following Key Security Indicators & Validations have been retired because they were replaced by a separate set of requirements and recommendations included in a specific FedRAMP standard (these will live on as empty indicators during Phase Two).

KSI-MLA-04:

- Previous: *Perform authenticated vulnerability scanning on information resources*
- Updated: **Superseded by KSI-MLA-03**

KSI-MLA-06:

- Previous: *Centrally track and prioritize the mitigation and/or remediation of identified vulnerabilities*
- Updated: **Superseded by KSI-MLA-03**

KSI-TPR-02:

- Previous: *Regularly confirm that services handling federal information or are likely to impact the confidentiality, integrity, or availability of federal information are FedRAMP authorized and securely configured*
- Updated: **Superseded by KSI-TPR-01**

Updates to Key Security Indicators & Validations

The following Key Security Indicators & Validations have been updated with different text to refine, clarify, or extend the requirement.

KSI-CED-01:

- Previous: Ensure all employees receive security awareness training
- Updated: Ensure all employees receive security **and privacy** awareness training**, incident response training, and are familiar with all relevant policies and procedures.**

KSI-CMT-01:

- Previous: Log and monitor system modifications
- Updated: Log and monitor **service** modifications

KSI-CMT-03:

- Previous: Implement automated testing and validation of changes *prior to deployment*
- Updated: Implement **persistent** automated testing and validation of changes

KSI-CMT-04:

- Previous: *Have* a documented change management procedure

- Updated: **Consistently follow** a documented change management procedure

KSI-CNA-01:

- Previous: Configure ALL information resources to limit inbound and outbound traffic
- Updated: Configure ALL **machine-based** information resources to limit inbound and outbound traffic

KSI-CNA-05:

- Previous: *Have* denial of service *protection*
- Updated: **Protect against** denial of service **attacks and unwanted spam**

KSI-IAM-05:

- Previous: *Apply zero trust design principles*
- Updated: **Design identity and access management systems that assume resources will be compromised**

KSI-INR:

- Previous: Incident *Reporting*
- Updated: Incident **Response**

KSI-INR-01:

- Previous: *Report* incidents according to FedRAMP requirements and cloud service provider policies
- Updated: **Respond to** incidents according to FedRAMP requirements and cloud service provider policies

KSI-MLA-03:

- Previous: Rapidly detect and *remediate or mitigate vulnerabilities*
- Updated: Rapidly detect and **respond to vulnerabilities following requirements and recommendations in the FedRAMP Vulnerability Response and Detection standard**

KSI-PIY-01:

- Previous: *Have an up-to-date information resource inventory or code defining all deployed assets, software, and services*
- Updated: **Generate inventories of information resources from authoritative sources**

KSI-PIY-02:

- Previous: *Have policies outlining the* security objectives *of all information resources*
- Updated: **Document the** security objectives **and requirements for each information resource**

KSI-PIY-04:

- Previous: Build security considerations into the Software Development Lifecycle and align with CISA Secure By Design principles
- Updated: Build security **and privacy** considerations into the Software Development Lifecycle and align with CISA Secure By Design principles

KSI-PIY-06:

- Previous: Have *a dedicated staff* and budget for security *with executive support,* commensurate with the size, complexity, scope, and risk of the service offering

- Updated: Have **staff and budget for security** commensurate with the size, complexity, scope, **executive priorities**, and risk of the service offering **that demonstrates commitment to delivering a secure service.**

KSI-SVC-01:

- Previous: *Harden and review network and system configurations*
- Updated: **Continuously evaluate machine-based information resources for opportunities to improve security**

KSI-SVC-03:

- Previous: Encrypt *all federal and sensitive* information at rest
- Updated: Encrypt information at rest **by default**

KSI-SVC-04:

- Previous: Manage configuration *centrally*
- Updated: Manage configuration **of machine-based information resources using automation**

KSI-SVC-05:

- Previous: *Enforce system and information resource integrity through cryptographic means*
- Updated: **Use cryptographic methods to validate the integrity of machine-based information resources**

KSI-TPR-01:

- Previous: *Identify all third-party information resources*

- Updated: **Follow the requirements and recommendations in the FedRAMP Minimum Assessment Standard regarding third-party information resources**

New Key Security Indicators & Validations

Low

The following Key Security Indicators & Validations have been created that affect the Low (and Moderate) baseline.

KSI-CED-03:

- Require role-specific training for development and engineering staff covering best practices for delivering secure software.
- Applies to: Low, Moderate

KSI-IAM-07

- Securely manage the lifecycle and privileges of all accounts, roles, and groups.
- Applies to: Low, Moderate

KSI-MLA-07

- Maintain a list of information resources and event types that will be monitored, logged, and audited.
- Applies to: Low, Moderate

Moderate

The following Key Security Indicators & Validations have been created that affect the Moderate baseline:

KSI-CNA-08

- Use automated services to persistently assess the security posture of all services and automatically enforce secure operations.
- Applies to: Moderate

KSI-MLA-08

- Use a least-privileged, role and attribute-based, and just-in-time access authorization model for access to log data.
- Applies to: Moderate

KSI-SVC-08

- Ensure that changes do not introduce or leave behind residual elements that could negatively affect confidentiality, integrity, or availability of information resources.
- Applies to: Moderate

KSI-SVC-09

- Use mechanisms that continuously validate the authenticity and integrity of communications between information resources.
- Applies to: Moderate

KSI-SVC-10

- Remove unwanted information promptly, including from backups if appropriate.
- Applies to: Moderate

Reference: Moderate Control Mappings for KSIs

The following list is intended to aid in automated comparison and review of Moderate control mappings.

KSI-CED-01, AT-2, AT-2.2, AT-2.3, AT-3.5, AT-4, IR-2.3

KSI-CED-02, AT-2, AT-2.3, AT-3, SR-11.1

KSI-CED-03, CP-3, IR-2, PS-6

KSI-CMT-01, AU-2, CM-3, CM-3.2, CM-4.2, CM-6, CM-8.3, MA-2

KSI-CMT-02, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8.1, SI-3

KSI-CMT-03, CM-3, CM-3.2, CM-4.2, SI-2

KSI-CMT-04, CM-3, CM-3.2, CM-3.4, CM-5, CM-7.1, CM-9

KSI-CMT-05, CA-7.4, CM-3.4, CM-4, CM-7.1, SI-2

KSI-CNA-01, AC-17.3, CA-9, CM-7.1, SC-7.5, SI-8

KSI-CNA-02, AC-17.3, AC-18.1, AC-18.3, AC-20.1, CA-9, SC-7.3, SC-7.4, SC-7.5, SC-7.8, SC-8, SC-10, SI-10, SI-11, SI-16

KSI-CNA-03, AC-12, AC-17.3, CA-9, SC-4, SC-7, SC-7.7, SC-8, SC-10

KSI-CNA-04, CM-2, SI-3

KSI-CNA-05, SC-5, SI-8, SI-8.2

KSI-CNA-06,

KSI-CNA-07, AC-17.3, CM-2, PL-10

KSI-CNA-08, CA-2.1, CA-7.1

KSI-IAM-01, AC-2, IA-2, IA-2.1, IA-2.2, IA-2.8, IA-5, IA-8, SC-23

KSI-IAM-02, AC-2, AC-3, IA-2.1, IA-2.2, IA-2.8, IA-5.1, IA-5.2, IA-5.6, IA-6, SC-23

KSI-IAM-03, AC-2, AC-2.2, AC-4, AC-6.5, IA-3, IA-5.2, RA-5.5

KSI-IAM-04, AC-2, AC-2.1, AC-2.2, AC-2.3, AC-2.4, AC-2.6, AC-3, AC-4, AC-5, AC-6, AC-6.1, AC-6.2, AC-6.5, AC-6.7, AC-6.9, AC-6.10, AC-7, AC-17, AC-17.4, AC-20.1, AU-9.4, CM-5, CM-7, CM-7.2, CM-7.5, CM-9, IA-4, IA-4.4, IA-7, PS-2, PS-3, PS-4, PS-5, PS-6, PS-9, RA-5.5, SC-2, SC-23, SC-39

KSI-IAM-05, AC-2.5, AC-2.6, AC-3, AC-4, AC-6, AC-12, AC-14, AC-17, AC-17.1, AC-17.2, AC-17.3, AC-20, AC-20.1, CM-2.7, CM-9, IA-2, IA-3, IA-4, IA-4.4, IA-5.2, IA-5.6, IA-11, PS-2, PS-3, PS-4, PS-5, PS-6, SC-4, SC-20, SC-21, SC-22, SC-23, SC-39, SI-3

KSI-IAM-06, AC-2, AC-2.1, AC-2.3, AC-2.13, AC-7, PS-4, PS-8

KSI-IAM-07, AC-2.2, AC-2.3, AC-2.13, AC-6.7, IA-4.4, IA-12, IA-12.2, IA-12.3, IA-12.5

KSI-INR-01, IR-4, IR-4.1, IR-6, IR-6.1, IR-6.3, IR-7, IR-7.1, IR-8, IR-8.1, SI-4.5

KSI-INR-02, IR-3, IR-4, IR-4.1, IR-5, IR-8

KSI-INR-03, IR-3, IR-4, IR-4.1, IR-8

KSI-MLA-01, AC-17.1, AC-20.1, AU-2, AU-3, AU-3.1, AU-4, AU-5, AU-6.1, AU-6.3, AU-7, AU-7.1, AU-8, AU-9, AU-11, IR-4.1, SI-4.2, SI-4.4, SI-7.7

KSI-MLA-02, AC-2.4, AC-6.9, AU-2, AU-6, AU-6.1, SI-4, SI-4.4

KSI-MLA-03, AU-5, CA-5, CA-7, RA-5, RA-5.2, SA-22, SI-2, SI-2.2, SI-3, SI-5, SI-7.7, SI-10, SI-11

KSI-MLA-04,

KSI-MLA-05, CA-7, CM-2, CM-6, SI-7.7

KSI-MLA-06,

KSI-MLA-07, AC-2.4, AC-6.9, AC-17.1, AC-20.1, AU-2, AU-7.1, AU-12, SI-4.4, SI-4.5, SI-7.7

KSI-MLA-08, SI-11

KSI-PIY-01, CM-2.2, CM-7.5, CM-8, CM-8.1, CM-12, CM-12.1, CP-2.8

KSI-PIY-02, AC-1, AC-21, AT-1, AU-1, CA-1, CA-2, CM-1, CP-1, CP-2.1, CP-2.8, CP-4.1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PL-4, PL-4.1, PS-1, RA-1, RA-9, SA-1, SC-1, SI-1, SR-1, SR-2, SR-3, SR-11

KSI-PIY-03, RA-5.11

KSI-PIY-04, AC-5, AU-3.3, CM-3.4, PL-8, PM-7, SA-3, SA-8, SC-4, SC-18, SI-10, SI-11, SI-16

KSI-PIY-05,

KSI-PIY-06, AC-5, CA-2, CP-2.1, CP-4.1, IR-3.2, PM-3, SA-2, SA-3, SR-2.1

KSI-PIY-07, CA-7.4, SC-18

KSI-RPL-01, CP-2.3, CP-10

KSI-RPL-02, CP-2, CP-2.1, CP-2.3, CP-4.1, CP-6, CP-6.1, CP-6.3, CP-7, CP-7.1, CP-7.2, CP-7.3, CP-8, CP-8.1, CP-8.2, CP-10, CP-10.2

KSI-RPL-03, CM-2.3, CP-6, CP-9, CP-10, CP-10.2, SI-12

KSI-RPL-04, CP-2.1, CP-2.3, CP-4, CP-4.1, CP-6, CP-6.1, CP-9.1, CP-10, IR-3, IR-3.2

KSI-SVC-01, CM-7.1, CM-12.1, MA-2, PL-8, SC-7, SC-39, SI-2.2, SI-4, SR-10

KSI-SVC-02, AC-1, AC-17.2, CP-9.8, SC-8, SC-8.1, SC-13, SC-20, SC-21, SC-22, SC-23

KSI-SVC-03, AC-19.5, AC-20.2, AC-21, CM-12, CP-9.8, SC-13, SC-28, SC-28.1

KSI-SVC-04, AC-2.4, CM-2, CM-2.2, CM-2.3, CM-6, CM-7.1, PL-9, PL-10, SA-5, SI-5, SR-10

KSI-SVC-05, CM-2.2, CM-8.3, SC-13, SC-23, SI-7, SI-7.1, SR-10

KSI-SVC-06, AC-17.2, IA-5.2, IA-5.6, SC-12, SC-17

KSI-SVC-07, CA-7.4, RA-5, RA-7

KSI-SVC-08, SC-4
KSI-SVC-09, SC-23, SI-7.1
KSI-SVC-10, SI-12.3, SI-18.4
KSI-TPR-01, CA-3, CM-10, PS-7, SA-4.9
KSI-TPR-02, AC-21, CA-3, CM-12, PS-7, SA-2, SA-4, SA-4.1, SA-4.2, SA-4.9, SA-9, SA-9.2, SA-10, SA-11, SA-15
KSI-TPR-03, AC-20, RA-3.1, SA-9, SA-10, SA-11, SA-15.3, SA-22, SI-7.1, SR-5, SR-6
KSI-TPR-04, AC-20, CA-3, IR-6.3, PS-7, RA-5, SA-9, SI-5, SR-5, SR-6, SR-8